United States Government Accountability Office

GAO

Report to Congressional Requesters

October 2008

DEFENSE CRITICAL INFRASTRUCTURE

Developing Training Standards and an Awareness of Existing Expertise Would Help DOD Assure the Availability of Critical Infrastructure

GAO-09-42

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defense Critical Infrastructure. Developing Training Standards and an Awareness of Existing Expertise Would Help DOD Assure the Availability of Critical Infrastructure	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Government Accountability Office,441 G Street NW,Washington,DC,20548**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**27**	

October 2008

DEFENSE CRITICAL INFRASTRUCTURE

Developing Training Standards and an Awareness of Existing Expertise Would Help DOD Assure the Availability of Critical Infrastructure

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-09-42, a report to congressional requesters

Why GAO Did This Study

The Department of Defense (DOD) relies on a global network of DOD and non-DOD infrastructure so critical that its unavailability could have a debilitating effect on DOD's ability to project, support, and sustain its forces and operations worldwide. DOD established the Defense Critical Infrastructure Program (DCIP) to assure the availability of mission-critical infrastructure. GAO was asked to evaluate the extent to which DOD has (1) incorporated aspects of DCIP into its exercises in the Transportation Defense Sector and (2) developed DCIP training standards departmentwide and made installation personnel aware of existing DCIP expertise. GAO examined a nonprojectable sample of 46 critical assets representing the four military services, five combatant commands, and selected installations within five defense sectors. GAO reviewed relevant DOD DCIP guidance and documents and interviewed cognizant officials regarding DCIP exercises, training, and awareness.

What GAO Recommends

GAO recommends that DOD (1) develop departmentwide DCIP training standards and an implementation time frame and (2) develop an effective means to communicate to installation personnel the existence and availability of DCIP expertise at the combatant command and military service levels. DOD concurred with both recommendations.

To view the full product, including the scope and methodology, click on GAO-09-42. For more information, contact Davi M. D'Agostino at (202) 512-5431 or dagostinod@gao.gov.

What GAO Found

U.S. Transportation Command (TRANSCOM) and the installations GAO visited that have critical transportation assets have incorporated aspects of critical infrastructure assurance into their exercises. DOD's DCIP guidance requires the combatant commands and the military services to conduct annual DCIP exercises, either separately or in conjunction with existing exercises. DCIP guidance also requires commanders to ensure submission of lessons learned from these exercises. For example, TRANSCOM has included aspects of critical infrastructure assurance in its two major biennial exercises. Although military personnel at 13 of the 19 installations GAO visited that have critical transportation assets generally were not aware of DCIP, GAO found that all 19 of these installations conduct routine exercises that often involve aspects of critical infrastructure assurance, and they incorporate lessons learned from past exercises into future exercises. For example, personnel at these installations conduct antiterrorism, emergency management, and continuity of operations planning exercises that often include critical assets located on the installation.

While several of the combatant commands and military services included in GAO's review of the five defense sectors have independently developed DCIP training at the headquarters level, DOD has not yet developed DCIP training standards departmentwide, and installation personnel remained largely unaware of existing DCIP expertise. DOD's DCIP instruction requires the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD[HD&ASA]) to provide policy and guidance for DCIP and oversee the implementation of DCIP education, training, and awareness of goals and objectives. ASD(HD&ASA) recognizes the need for DCIP training and program awareness, as noted in its March 2008 critical infrastructure strategy. However, given the newness of the strategy, ASD(HD&ASA) has not yet established departmentwide DCIP training standards for assuring the availability of critical infrastructure or a time frame for implementing the training standards. In the absence of established DCIP training standards, the combatant commands and military services are variously developing and implementing their own DCIP training programs. For example, the Navy has established an information assurance training program that includes a DCIP module. Furthermore, installation personnel GAO spoke with, with few exceptions, were not familiar with DCIP or aware of DCIP expertise at the combatant command and military service headquarters levels. In addition, DOD has not developed an effective way to communicate to installation personnel the existence of DCIP expertise. Consequently, they rely on other, more established programs that in some cases do not emphasize the consideration of the full spectrum of threats and hazards. Without DCIP training standards departmentwide and a means of communicating them to installation personnel, the combatant commands and military services potentially may develop mutually redundant or inconsistent training programs, and installation personnel will continue to be unaware of existing DCIP expertise.

Contents

Abbreviations

AFB	air force base
ASD(HD&ASA)	Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
CENTCOM	U.S. Central Command
DCIP	Defense Critical Infrastructure Program
DOD	Department of Defense
GIG	Global Information Grid
ISR	Intelligence, Surveillance, and Reconnaissance
OSD	Office of the Secretary of Defense
PACOM	U.S. Pacific Command
TRANSCOM	U.S. Transportation Command

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

October 30, 2008

The Honorable Solomon P. Ortiz
Chairman
The Honorable J. Randy Forbes
Ranking Member
Subcommittee on Readiness
Committee on Armed Services
House of Representatives

The Honorable W. Todd Akin
House of Representatives

The Department of Defense (DOD) relies on a global network of DOD- and non-DOD-owned critical infrastructure to carry out its missions, and the incapacitation or destruction of one or more of the assets constituting this network could have a debilitating effect on DOD's ability to project, support, and sustain its forces and operations worldwide. Because of its importance to DOD operations, this critical infrastructure represents an attractive target to adversaries and may also be vulnerable to a host of natural disasters and accidents. In September 2003, the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD[HD&ASA]) was assigned responsibility for DOD's critical infrastructure protection efforts. ASD(HD&ASA) subsequently issued guidance in August 2005 establishing the Defense Critical Infrastructure Program (DCIP) to assure the availability of mission-critical infrastructure and articulating the roles and responsibilities for DOD organizations involved in the program.[1] Under DCIP, DOD created 10 functionally based defense sectors and designated a Defense Infrastructure Sector Lead Agent (hereinafter referred to as sector lead agent) for each sector.[2] DOD also created several other complementary programs, including the Antiterrorism Program,[3] established to protect

[1]DOD Directive 3020.40, *Defense Critical Infrastructure Program (DCIP)* (Washington, D.C.: Apr. 19, 2005).

[2]The 10 defense sectors are the Defense Industrial Base; Financial Services; Global Information Grid; Health Affairs; Intelligence, Surveillance, and Reconnaissance; Logistics; Personnel; Public Works; Space; and Transportation.

[3]DOD Directive 2000.12, *DOD Antiterrorism (AT) Program* (Washington, D.C.: Aug. 18, 2003 (certified current as of Dec. 13, 2007)).

DOD assets and personnel from terrorist acts, and the Information Assurance Program,[4] established to protect and defend DOD information and information systems. Both programs predate DCIP, yet they contribute indirectly to the protection and assurance of critical assets. Although not the focus of this report, these complementary programs indirectly support elements of DCIP.

In response to your request, we have thus far issued six reports since May 2007. Our first report examined the extent to which DOD has developed a comprehensive management plan for DCIP and the actions needed to identify, prioritize, and assess defense critical infrastructure.[5] The second report examined DOD's efforts to implement a risk management approach for defense industrial base critical assets.[6] The third report examined the extent to which DOD included highly sensitive assets in its critical infrastructure program.[7] The fourth report focused on threats and vulnerabilities affecting intelligence, surveillance, and reconnaissance (ISR) operations at Creech Air Force Base, Nevada.[8] The fifth report focused on DOD's efforts to assure the availability of critical assets in the Transportation Defense Sector.[9] Finally, the sixth report focused on DOD's efforts to assure the availability of critical infrastructure in the Space, ISR, and Global Information Grid (GIG) Defense Sectors (referred to as the

[4]DOD Directive 8500.01E, *Information Assurance (IA)* (Washington, D.C.: Oct. 24, 2002 (certified current as of Apr. 23, 2007)).

[5]GAO, *Defense Infrastructure: Actions Needed to Guide DOD's Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure*, GAO-07-461 (Washington, D.C.: May 24, 2007).

[6]GAO, *Defense Infrastructure: Management Actions Needed to Ensure Effectiveness of DOD's Risk Management Approach for the Defense Industrial Base*, GAO-07-1077 (Washington, D.C.: Aug. 31, 2007).

[7]GAO, *Defense Critical Infrastructure: DOD's Risk Analysis of Its Critical Infrastructure Omits Highly Sensitive Assets*, GAO-08-373R (Washington, D.C.: Apr. 2, 2008).

[8]GAO, *Defense Critical Infrastructure: Additional Air Force Actions Needed at Creech Air Force Base to Ensure Protection and Continuity of UAS Operations*, GAO-08-469RNI (Washington, D.C.: Apr. 23, 2008) (For Official Use Only).

[9]GAO, *Defense Critical Infrastructure: Adherence to Guidance Would Improve DOD's Approach to Identifying and Assuring the Availability of Critical Transportation Assets*, GAO-08-851 (Washington, D.C.: Aug. 15, 2008).

Tri-Sector throughout this report).[10] All of our related products are listed in the Related GAO Products section at the end of this report.

In 2007, we reported that DCIP implementation at the department, military service, and combatant command headquarters levels was relatively immature.[11] To determine the status of DOD's efforts regarding DCIP training and exercises, this report examines the extent to which DOD has (1) incorporated aspects of DCIP into its exercises in the Transportation Defense Sector and (2) developed DCIP training standards departmentwide and made installation personnel aware of existing DCIP expertise. Our recent work examining the assurance of critical infrastructure focused on 5 of the 10 defense sectors: GIG, ISR, Public Works, Space, and Transportation. This report's objective examining the extent to which DOD has incorporated aspects of DCIP into its exercises in the Transportation Defense Sector focused on DCIP-related exercises conducted by U.S. Transportation Command (TRANSCOM) and on exercises conducted at individual installations we visited that have critical transportation assets. For our second objective, the scope of our work on the extent to which DOD has developed DCIP training standards departmentwide and made installation personnel aware of existing DCIP expertise focused on efforts at the Office of the Secretary of Defense (OSD); at the four military services; within five combatant commands—U.S. Central Command (CENTCOM), U.S. European Command, U.S. Pacific Command (PACOM), U.S. Strategic Command, and TRANSCOM; and at selected installations that have critical assets representing each of the five defense sectors that we visited. Regarding DCIP awareness, the scope of our work focused on installation personnel who are responsible for critical transportation assets.

We drew a nonprobability sample[12] of critical assets in the United States and abroad, using draft critical asset lists developed by the Joint Staff, each of the four military services, TRANSCOM, the Defense Intelligence Agency, and the Defense Information Systems Agency. We selected assets

[10]GAO, *Defense Critical Infrastructure: DOD's Evolving Assurance Program Has Made Progress but Leaves Critical Space, Intelligence, and Global Communications Assets at Risk*, GAO-08-828NI (Washington, D.C.: Aug. 22, 2008) (For Official Use Only).

[11]GAO-07-461.

[12]Results from nonprobability samples cannot be used to make inferences about a population, because in a nonprobability sample some elements of the population being studied have no chance or an unknown chance of being selected as part of the sample.

for our review based on the following criteria: (1) overlap among the various critical asset lists; (2) geographic dispersion among geographic combatant commands' areas of responsibility; (3) representation from each military service; and (4) with respect to transportation assets, representation in TRANSCOM's three asset categories: air bases, seaports, and commercial airports. Using this methodology, we selected 46 total critical assets for review—22 transportation assets[13] and 24 Tri-Sector assets—in the United States and in Europe, the Middle East, and the Pacific region.[14]

Further, we reviewed relevant DOD guidance pertaining to DCIP training and exercise requirements and interviewed officials from OSD, the Joint Staff, defense agencies, the military services, combatant commands, and sector lead agents responsible for DCIP. (Throughout this unclassified report, we do not identify the 46 specific critical assets, their locations or installations, or combatant command or others' missions that the assets support because that information is classified.) We conducted this performance audit from May 2007 through September 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. A more thorough description of our scope and methodology is provided in appendix I.

Results in Brief

TRANSCOM and the installations we visited that have critical transportation assets have incorporated aspects of critical infrastructure assurance into their exercises. DOD's guidance requires the testing of antiterrorism and continuity of operation plans annually through various exercises. DOD's antiterrorism guidance requires that commanders maintain antiterrorism exercise documentation for no less than 2 years to ensure incorporation of lessons learned. For example, TRANSCOM has included aspects of critical infrastructure assurance in its two major

[13]For purposes of this report, we are including only 19 installations that have critical transportation assets, since the remaining three critical transportation assets in our sample are commercial airports that have no DOD personnel stationed at them.

[14]For greater detail on asset selection methodology, see GAO-08-851 and GAO-08-828NI (For Official Use Only).

biennial battle staff exercises. Although military personnel with whom we spoke at installations we visited that have critical transportation assets generally were not aware of DCIP, we found that these installations conduct routine exercises that often involve critical infrastructure assurance, and they incorporate lessons learned from past exercises into plans for future exercises. For example, personnel at these installations conduct antiterrorism, emergency management, and continuity of operations planning exercises that often include critical assets located on the installation.

While several of the combatant commands and military services included in our review of the five defense sectors have independently developed DCIP training at the headquarters level, DOD has not yet developed DCIP training standards departmentwide, and installation personnel remained largely unaware of existing DCIP expertise. DOD's DCIP instruction, issued in 2008, requires ASD(HD&ASA) to provide policy and guidance for DCIP and oversee the implementation of DCIP education, training, and awareness of goals and objectives. ASD(HD&ASA) recognizes the need for DCIP training and program awareness, as noted in its March 2008 critical infrastructure strategy. However, given the newness of the strategy, ASD(HD&ASA) has not yet established departmentwide DCIP training standards for assuring the availability of critical infrastructure or a time frame for implementing the training standards. In the absence of established DCIP training standards, the combatant commands and military services are variously developing and implementing their own DCIP training programs. For example, PACOM officials stated that they have conducted internal PACOM training and education on critical infrastructure assurance. The Department of the Navy has established an information assurance training program that includes a DCIP module. Furthermore, installation personnel we spoke with who are responsible for assuring the availability of critical transportation assets, with few exceptions, were not familiar with DCIP or aware of DOD's critical infrastructure expertise at the combatant command and military service headquarters levels for two reasons. First, as we previously reported, the military services have not yet developed specific guidance for how installations are to implement DCIP. Second, DCIP efforts to date have focused primarily on the identification and assessment of critical infrastructure. In addition, DOD has not developed an effective way to communicate to installation personnel the existence of DCIP expertise. Consequently, installation personnel responsible for assuring the availability of defense critical infrastructure rely on other, more established programs, such as the Antiterrorism Program, that in some cases do not emphasize consideration of the full spectrum of threats and

hazards, such as earthquakes and typhoons. Without DCIP training standards departmentwide, the combatant commands and military services potentially may develop mutually redundant or inconsistent training programs. Furthermore, installation personnel will continue to have limits to their awareness of DCIP knowledge, which will affect how they assure the availability of critical infrastructure.

We are recommending that Secretary of Defense direct ASD(HD&ASA) to develop departmentwide DCIP training standards and an implementation time frame and to coordinate with the combatant commands and the military services to develop a way to effectively communicate to installation personnel the existence of DCIP expertise and availability.

We provided a draft of this report to DOD in September 2008 for its review and comment. In written comments on a draft of this report, DOD concurred with both of our recommendations. Also, TRANSCOM provided us with technical comments, which we incorporated in the report as appropriate. DOD's response is reprinted in appendix II.

Background

ASD(HD&ASA), within the Office of the Under Secretary of Defense for Policy, serves as the principal civilian advisor and the Chairman of the Joint Chiefs of Staff serves as the principal military advisor to the Secretary of Defense on critical infrastructure protection.

ASD(HD&ASA) has issued guidance to help assure the availability of critical infrastructure. A component of this guidance outlines the roles and responsibilities of the organizations involved in DCIP. Table 1 summarizes the training and exercise roles and responsibilities of each DCIP organization.

Table 1: DCIP Training and Exercise Roles and Responsibilities

DCIP organization	DCIP guidance	
	DOD Directive 3020.40	DOD Instruction 3020.45[a]
ASD(HD&ASA)	• Ensure the implementation of DCIP education, training, and awareness activities in coordination with the Chairman of the Joint Chiefs of Staff.	• Provide policy and guidance for DCIP and oversee (including but not limited to) the implementation of education, training, and awareness goals and objectives.
Chairman of the Joint Chiefs of Staff	• Integrate DCIP functions and activities into joint planning, doctrine, training, and exercises. • Assist ASD(HD&ASA) in the development and maintenance of DCIP standards and procedures. • Review DCIP-related doctrine, standards, procedures, and training of combatant commands and military departments.	
Military departments	• Incorporate DCIP elements into education and training programs, including the testing and exercising of mitigation and response plans.	• Implement training and education activities designed to meet DCIP education and training goals and objectives. • Execute annual exercises, either separately or in conjunction with existing exercises, to integrate other federal departments and agencies in the risk reduction and in the protection, recovery, and restoration of defense critical infrastructure notionally affected by the full spectrum of threats and hazards. • Direct the incorporation of DCIP plans into joint operations, training, and exercises. Commanders shall ensure the submission of DCIP lessons learned.
Combatant commands		• Develop and exercise defense critical infrastructure mitigation plans to demonstrate that continuity of operations can be maintained. • Execute annual exercises, either separately or in conjunction with existing exercises, to integrate other federal departments and agencies in the risk reduction and in the protection, recovery, and restoration of defense critical infrastructure notionally affected by the full spectrum of threats and hazards. • Direct the incorporation of DCIP plans into joint operations, training, and exercises. Commanders shall ensure the submission of DCIP lessons learned.

Source: GAO analysis of DOD DCIP guidance.

[a]DOD Instruction 3020.45, *Defense Critical Infrastructure Program (DCIP) Management* (Washington, D.C.: Apr. 21, 2008).

Aspects of Critical Infrastructure Assurance Are Incorporated into TRANSCOM and Installation Exercises

TRANSCOM Incorporates Critical Infrastructure Protection into Its Exercises

In its role as a combatant command, TRANSCOM incorporates critical infrastructure protection-related events into its two major biennial battle staff exercise programs. Turbo Challenge and Turbo Distribution are TRANSCOM-sponsored exercises that test and evaluate the capability of the Defense Transportation System to support the deployment and sustainment of forces associated with a particular combatant command operation plan or the movement of personnel and cargo in response to a crisis.

TRANSCOM officials told us that the objective of including critical infrastructure protection-related events in its major exercises is to evaluate the command's response to threats, loss, or degradation of its critical infrastructure. TRANSCOM also evaluates the potential to include critical infrastructure-related events in other combatant command exercises that it supports.

TRANSCOM and the installations we visited that have critical transportation assets have incorporated DCIP-like elements into their existing exercises. Although installation personnel we met with often were unaware of DCIP, we found that many conducted routine antiterrorism, emergency management, information assurance, and continuity of operations planning exercises that often include critical transportation assets located on the installation.

As part of their regularly scheduled antiterrorism and continuity of operations programs, installation officials at all 19 installations we visited that have critical transportation assets conducted exercises encompassing critical assets located on their installations. However, unlike DCIP, some of these programs do not emphasize an all-threats, all-hazards approach to assuring critical infrastructure. DOD guidance requires the testing of antiterrorism[15] and continuity of operations[16] plans annually through various exercises. DOD's antiterrorism guidance requires that commanders maintain antiterrorism exercise documentation for no less than 2 years to ensure incorporation of lessons learned. These antiterrorism exercises often contain aspects of DCIP, such as (1) developing adaptive plans and procedures to mitigate risk, (2) restoring capability in the event of a loss or degradation of assets, (3) supporting incident management, and (4) protecting critical infrastructure-related sensitive information. For example, even though installation personnel are often unaware of DCIP, we found that exercises testing antiterrorism and continuity of operations plans typically include critical installation infrastructure, and exercises for emergency management plans sometimes include assuring the availability of critical transportation assets in the event of natural disasters. Several installations in Japan that we visited conducted exercises that assure the availability of critical transportation assets located on those installations. Also, several installation officials responsible for critical transportation assets in PACOM's area of responsibility with whom we met told us that they conduct exercises that examine the impact of natural disasters, such as earthquakes and typhoons, on critical infrastructure. Installation officials responsible for critical transportation assets in CENTCOM's area of responsibility told us that they incorporate lessons learned into future

[15]DOD Instruction 2000.16, *DOD Antiterrorism (AT) Standards* (Washington, D.C.: Oct. 2, 2006).

[16]DOD Directive 3020.26, *Defense Continuity Program (DCP)* (Washington, D.C.: Sept. 8, 2004).

exercises. For instance, an installation in the Middle East used exercises to prepare for its response to and recovery from major accidents, natural disasters, attacks, or terrorist use of chemical, biological, radiological, nuclear, or high-yield explosives, and has incorporated its findings into planning for future exercises.

DOD Has Not Developed DCIP Training Standards Departmentwide, and Installation Personnel Remain Unaware of Existing DCIP Expertise

Although several of the combatant commands and military services we visited have variously developed headquarters-level DCIP training programs, DOD has not developed DCIP training standards departmentwide. Further, many of the installation personnel responsible for the assurance of critical infrastructure remain unaware of the DCIP program and the DCIP expertise available at the combatant command and military service levels.

DCIP Training Standards Have Not Yet Been Developed Departmentwide

DOD's DCIP instruction requires ASD(HD&ASA) to provide policy and guidance for DCIP and oversee the implementation of DCIP education, training, and awareness of goals and objectives. ASD(HD&ASA) recognized the need for DCIP training in its March 2008 Strategy for Defense Critical Infrastructure.[17] Specifically, the strategy states that ASD(HD&ASA) will establish baseline critical infrastructure education requirements. Given that this strategy is relatively new, DCIP training standards have not yet been established departmentwide nor has DOD established a time frame for implementing the training standards. However, in the absence of DCIP training standards departmentwide, we determined through our work examining the five defense sectors that several combatant commands and military services have independently developed their own training programs or modules. For example, PACOM officials stated that they have conducted internal PACOM training and education on critical infrastructure assurance. U.S. Strategic Command has conducted internal training and continuous education for its staff.

[17]Department of Defense, *Strategy for Defense Critical Infrastructure* (Washington, D.C.: March 2008).

Further, TRANSCOM and CENTCOM officials told us that they have developed critical infrastructure training for their headquarters-level personnel. Additionally, CENTCOM officials told us that the development of their internal critical infrastructure training was still in its initial stages. Conversely, U.S. European Command officials told us that they are currently focused almost exclusively on identifying critical infrastructure and threats to those assets.

Moreover, the Department of the Navy has developed a DCIP training module that it has incorporated into its information assurance training.[18] The module provides an overview of critical infrastructure protection and the vulnerabilities created by increased interdependencies. The U.S. Marine Corps has begun familiarizing its installation antiterrorism officers with DCIP through required training for its Critical Asset Management System, used by the U.S. Marine Corps to track critical infrastructure. Air Force officials told us that they have a mission assurance training module that includes critical infrastructure protection, and like the U.S. Marine Corps, they conduct training for major Air Force commands on their version of the Critical Asset Management System. Further, officials we spoke with at the Air Mobility Command—an Air Force major command and subcomponent command to TRANSCOM—told us that they provide annual DCIP training to their air mobility wings. Army officials we met with did not identify Army-specific DCIP training but stated that training needs to be comprehensive and not defense sector specific.

However, because there are no DCIP training standards departmentwide and combatant command- and military service-level training has not reached installation personnel responsible for assuring the availability of defense critical infrastructure, installation personnel rely on other, more established programs, such as the Antiterrorism Program. However, unlike DCIP, some of these programs do not emphasize consideration of the full spectrum of threats and hazards that can compromise the availability of critical infrastructure.[19] For example, the Antiterrorism Program focuses on terrorist threats to assets and personnel. While some DCIP training exists, the combatant commands' and military services' development of disparate training programs, without benefit of DCIP training standards

[18]DOD Information Assurance Awareness version 6.0.

[19]A threat is an adversary having the intent, capability, and opportunity to cause loss or damage, while hazards are defined as non-hostile incidents, such as accidents, natural forces, and technological failures, that cause loss or damage to infrastructure assets.

departmentwide, may result in programs that contain potentially conflicting information. As a result, training may be less effective, and resources may be used inefficiently.

With Few Exceptions, Installation Personnel We Met with Responsible for Critical Transportation Assets Were Unaware of Existing DCIP Expertise

With few exceptions, installation personnel we met with who are responsible for assuring the availability of critical transportation infrastructure were not familiar with DCIP and were not aware that the combatant commands or military services possessed DCIP expertise that they could leverage for two reasons. First, as we previously reported,[20] the military services have not yet developed specific guidance for how installations are to implement DCIP. Second, DCIP efforts to date have focused primarily on the identification and assessment of critical infrastructure. At 13 of the 19 installations we visited that have critical transportation assets, installation personnel we spoke with stated that prior to our visit, they had not heard of DCIP. Furthermore, DOD has not developed an effective way to communicate that DCIP expertise is available to installation personnel at the combatant command and military service levels. Until DOD develops a way to effectively communicate the existence of DCIP expertise to installation personnel, such personnel may not be able to fully leverage DCIP knowledge, which will affect how they assure the availability of critical infrastructure from an all-hazards approach, which they currently may not be doing.

Conclusions

Because the network of DOD- and non-DOD-owned critical infrastructure represents an attractive target to adversaries and also is potentially vulnerable to a variety of natural disasters or accidents, it is crucial for DOD to conduct DCIP exercises and develop and implement DCIP training. With few exceptions, at the sites we visited, installation officials responsible for the assurance of critical assets were not aware of DCIP. However, they conducted complementary exercises that while in some cases not emphasizing the full spectrum of threats and hazards, often involved some aspects of critical infrastructure assurance and provided a measure of protection for critical assets located on the installation. In the absence of DCIP training standards departmentwide, the combatant commands and military services are developing and implementing disparate training programs, which may result in duplicative programs or programs that potentially may contain inconsistent information. As a

[20] GAO-07-461.

result, training may be less effective and resources may be used inefficiently. Furthermore, lacking a process for communicating existing DCIP expertise across the department, installation personnel will be unable to take full advantage of existing knowledge in assuring the availability of critical infrastructure.

Recommendations for Executive Action

We are making two recommendations to help assure the availability of critical infrastructure by improving training and awareness. We recommend that the Secretary of Defense direct ASD(HD&ASA) to:

- Develop departmentwide DCIP training standards and an implementation time frame to enable the combatant commands and military services to develop consistent and cost-effective training programs.
- Coordinate with the combatant commands and military services to develop an effective means to communicate to installation personnel the existence and availability of DCIP expertise at the combatant command and military service levels.

Agency Comments

In written comments on a draft of this report, DOD concurred with both of our recommendations. Also, TRANSCOM provided us with technical comments, which we incorporated in the report where appropriate. DOD's comments are reprinted in appendix II.

DOD concurred with our recommendation to develop departmentwide DCIP training standards and an implementation time frame to enable the combatant commands and military services to develop consistent and cost-effective training programs. In its comments, DOD stated that ASD(HD&ASA) intends to designate U.S. Joint Forces Command as the executive agent for the development of critical infrastructure protection education and training standards, and upon completion of the development of training standards, ASD(HD&ASA) will set a 180-day time frame for full implementation by the combatant commands and military services to enable consistent and cost-effective training.

DOD also concurred with our recommendation to coordinate with the combatant commands and military services to develop an effective means to communicate to installation personnel the existence and availability of DCIP expertise at the combatant command and military service levels. DOD noted that ASD(HD&ASA) intends to take steps to make critical infrastructure protection materials available to installation personnel and will continue to work with the Joint Staff, U.S. Joint Forces Command, and the Defense Threat Reduction Agency to develop an effective means

to improve communication regarding the availability of critical infrastructure protection expertise.

We are sending copies of this report to the Chairmen and Ranking Members of the Senate and House Committees on Appropriations, Senate and House Committees on Armed Services, and other interested congressional parties. We also are sending copies of this report to the Secretary of Defense; the Chairman of the Joint Chiefs of Staff; the Secretaries of the Army, the Navy, and the Air Force; the Commandant of the U.S. Marine Corps; the combatant commanders of the functional and geographic combatant commands; the Commander, U.S. Army Corps of Engineers; the Director, Defense Intelligence Agency; the Director, Defense Information Systems Agency; and the Director, Office of Management and Budget. We will also make copies available to others upon request. This report will also be available at no charge on GAO's Web site at http://www.gao.gov.

If you or your staff have questions concerning this report, please contact me at (202) 512-5431 or dagostinod@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.

Davi M. D'Agostino
Director, Defense Capabilities and
Management

Appendix I: Scope and Methodology

To determine the extent to which the Department of Defense (DOD) has (1) incorporated aspects of the Defense Critical Infrastructure Program (DCIP) into its exercises in the Transportation Defense Sector and (2) developed DCIP training standards departmentwide and made installation personnel aware of existing DCIP expertise, we obtained relevant documentation and interviewed officials from the following DOD organizations:[1]

- Office of the Secretary of Defense (OSD)
  - Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
- Joint Staff, Directorate for Operations, Antiterrorism and Homeland Defense
- Defense Threat Reduction Agency, Combat Support Assessments Division
- Military services
  - Department of the Army, Asymmetric Warfare Office, Critical Infrastructure Risk Management Branch
  - Department of the Navy
    - Office of the Chief Information Officer
    - Mission Assurance Division, Naval Surface Warfare Center, Dahlgren Division, Dahlgren, Virginia
  - Department of the Air Force, Air, Space and Information Operations, Plans, and Requirements, Homeland Defense Division
  - Headquarters, U.S. Marine Corps, Security Division, Critical Infrastructure Protection Office
- Combatant commands
  - Headquarters, U.S. Central Command, Critical Infrastructure Program Office, MacDill Air Force Base (AFB), Florida
  - Headquarters, U.S. European Command, Critical Infrastructure Protection Program Office, Patch Barracks, Vaihingen, Germany
  - Headquarters, U.S. Pacific Command, Antiterrorism and Critical Infrastructure Division, Camp H.M. Smith, Hawaii
    - U.S. Forces Japan
  - Headquarters, U.S. Transportation Command (TRANSCOM), Critical Infrastructure Program, Scott AFB, Illinois
    - Headquarters, Air Mobility Command, Homeland Defense Branch, Scott AFB, Illinois
  - Headquarters, U.S. Strategic Command, Mission Assurance Division, Offutt AFB, Nebraska

[1]DOD organizations are located in the Washington, D.C., metropolitan area unless otherwise indicated.

- Defense infrastructure sector lead agents
  - Headquarters, Defense Intelligence Agency, Critical Infrastructure Protection Team
  - Headquarters, Defense Information Systems Agency, Office for Critical Infrastructure Protection and Homeland Security/Defense
  - Headquarters, TRANSCOM, Critical Infrastructure Program, Scott AFB, Illinois
  - Headquarters, U.S. Strategic Command, Mission Assurance Division, Offutt AFB, Nebraska
  - Headquarters, U.S. Army Corps of Engineers, Directorate of Military Programs
- Selected critical assets in the continental United States, Hawaii, the U.S. Territory of Guam, Germany, Greece, Kuwait and another country in U.S. Central Command's area of responsibility, and Japan

We drew a nonprobability sample[2] of critical assets in the United States and abroad, using draft critical asset lists developed by the Joint Staff, each of the four military services, TRANSCOM, the Defense Intelligence Agency, and the Defense Information Systems Agency. We selected assets for our review based on the following criteria: (1) overlap among the various critical asset lists; (2) geographic dispersion among geographic combatant commands' areas of responsibility; (3) representation from each military service; and (4) with respect to transportation assets, representation in TRANSCOM's three asset categories: air bases, seaports, and commercial airports. Using this methodology, we selected 46 total critical assets for review—22 transportation assets[3] and 24 Tri-Sector assets—in the United States and in Europe, the Middle East, and the Pacific region.[4]

Further, we reviewed relevant DOD guidance pertaining to DCIP training and exercise requirements and interviewed officials from OSD, the Joint Staff, defense agencies, the military services, the combatant commands, and the defense infrastructure sector lead agents responsible for DCIP.

[2]Results from nonprobability samples cannot be used to make inferences about a population, because in a nonprobability sample some elements of the population being studied have no chance or an unknown chance of being selected as part of the sample.

[3]For purposes of this report, we are including only 19 installations that have critical transportation assets, since the remaining three critical transportation assets in our sample are commercial airports that have no DOD personnel stationed at them.

[4]For greater detail on asset selection methodology, see GAO-08-851 and GAO-08-828NI (For Official Use Only).

(Throughout this unclassified report, we do not identify the 46 specific critical assets, their locations or installations, or combatant command or others' missions that the assets support because that information is classified.)

This report's first objective, examining the extent to which DOD has incorporated aspects of DCIP into its exercises in the Transportation Defense Sector, focused on DCIP-related exercises conducted by TRANSCOM and on exercises conducted at individual installations we visited that have critical transportation assets. To address this objective, we reviewed and analyzed policies, assurance plans, strategies, handbooks, directives, and instructions. Further, we spoke with installation personnel about their efforts to incorporate aspects of DCIP into installation exercises and reviewed and analyzed installation emergency management plans, information assurance plans, and continuity of operations plans to determine how, if at all, critical assets were incorporated into exercises. In addition, to determine how critical assets are included and how lessons learned are incorporated into future exercises, we interviewed combatant command, subcomponent, and installation personnel responsible for planning and conducting exercises involving critical assets.

For our second objective, the scope of our work on the extent to which DOD has developed DCIP training standards departmentwide and made installation personnel aware of existing DCIP expertise focused on efforts at OSD; at the four military services; within five combatant commands—U.S. Central Command, U.S. European Command, U.S. Pacific Command, U.S. Strategic Command, and TRANSCOM; and at installations that have critical assets representing each of the five defense sectors that we visited. Regarding DCIP awareness, the scope of our work focused exclusively on installation personnel who are responsible for critical transportation assets. To address this objective, we reviewed existing combatant command and military service DCIP training programs and interviewed program officials at the OSD, combatant command, and military service headquarters levels. Further, we interviewed installation personnel responsible for assuring the critical infrastructure we selected as part of our nonprobability sample to determine their awareness of DCIP and the existence of DCIP expertise and their ability to leverage these resources.

We conducted this performance audit from May 2007 through September 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for

our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Defense

HOMELAND DEFENSE
& AMERICAS' SECURITY AFFAIRS

ASSISTANT SECRETARY OF DEFENSE
2600 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-2600

OCT 16 2008

Ms. Davi M. D'Agostino
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. D'Agostino:

This is the Department of Defense (DoD) response to the GAO draft report, GAO-09-42, "DEFENSE CRITICAL INFRASTRUCTURE: Developing Training Standards and an Awareness of Existing Expertise Would Help DoD Assure the Availability of Critical Infrastructure," (GAO Code 351240). DoD concurs with the two recommendations in the report. Our response to your recommendations is enclosed.

Our point of contact for this action is Mr. Antwane Johnson, Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (OASD (HD&ASA)), (703) 602-5730, Extension 143 or Antwane.Johnson@osd.mil.

Sincerely,

Paul McHale
Peter F. Verga
Principal Deputy

Enclosure:
As stated

GAO DRAFT REPORT – DATED SEPTEMBER 24, 2008
GAO CODE 351240/GAO-09-42

"DEFENSE CRITICAL INFRASTRUCTURE: Developing Training Standards and an Awareness of Existing Expertise Would Help DoD Assure the Availability of Critical Infrastructure"

DEPARTMENT OF DEFENSE COMMENTS TO THE RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense direct the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs to develop Department-wide Defense Critical Infrastructure Program training standards and an implementation time frame to enable the combatant commands and Military Services to develop consistent and cost-effective training programs.

DOD RESPONSE: Concur. As noted in the March 2008 DCIP Strategy, OASD(HD&ASA) recognizes the need for DCIP training and program awareness. Given the newness of the strategy, and the fact that the Critical Asset Identification Process Manual is still in final coordination, OASD(HD&ASA) has not yet established Department-wide training standards. We recognize that several of the combatant commands and Military Services are independently developing and implementing their own DCIP training programs. OASD(HD&ASA) intends to designate United States Joint Forces Command (USJFCOM) as the executive agent for the development of critical infrastructure protection education and training standards. USJFCOM will be tasked to provide CIP education course curricula, and to develop program training standards to support both classroom-based instruction and web-based study. OASD(HD&ASA) will work with USJFCOM in developing and establishing minimum CIP education course criteria and training standards. Upon completion of the development of the materials, OASD (HD&ASA) will set a 180-day time frame for full implementation by the combatant commands and Military Services to enable consistent and cost-effective CIP training.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense direct the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs to coordinate with the combatant commands and Military Services to develop an effective means to communicate to installation personnel the existence and availability of Defense Critical Infrastructure Program expertise at the combatant command and Military Service levels.

DOD RESPONSE: Concur. As noted in the March 2008 DCIP Strategy, OASD(HD&ASA) recognizes the need for DCIP training and program awareness which is re-enforced in DoD Instruction 3020.45. The focus of the program to date has been on the combatant commands, the Military Services and the defense sectors. DCIP concepts and procedures have not yet reached installation personnel that own and operate the assets. As DCIP policy and procedures are being promulgated, the Military Services are beginning to develop their implementation guidance. The

Army has developed Service-specific guidance (AR 525-26) and HQDA is executing that guidance in support of DoD Directive 3020.40 and DoD Instruction 3020.45. The Air Force is developing a draft Air Force Instruction for CIP which is in the coordination process. The other Military Services prefer to await official publication of the Critical Asset Identification Process prior to implementing Service-specific guidance. OASD(HD&ASA) intends, as a part of the CIP training standards, to have appropriate CIP materials (brochures, flyers, web link) available for CIP awareness and education. These tools would be made available inside installation "welcome aboard packets" during indoctrination. In addition, OASD(HD&ASA) has developed in conjunction with the Defense Threat Reduction Agency (DTRA), a DCIP Introduction briefing to be used during Joint Staff sponsored Mobile Training Team seminars at combatant command and Service Antiterrorism and Force Protection training sessions. OASD(HD&ASA) will continue to work with the Joint Staff, JFCOM, and DTRA in developing an effective means to improve communication regarding the availability of CIP expertise.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Davi M. D'Agostino, (202) 512-5431 or dagostinod@gao.gov

Acknowledgments

In addition to the contact named above, Mark A. Pross, Assistant Director; Gina M. Flacco; James P. Krustapentus; Kate S. Lenane; Terry L. Richardson; Marc J. Schwartz; John S. Townes; Cheryl A. Weissman; and Alex M. Winograd made key contributions to this report.

Related GAO Products

Defense Critical Infrastructure: DOD's Evolving Assurance Program Has Made Progress but Leaves Critical Space, Intelligence, and Global Communications Assets at Risk. GAO-08-828NI. Washington, D.C.: August 22, 2008 (For Official Use Only).

Defense Critical Infrastructure: Adherence to Guidance Would Improve DOD's Approach to Identifying and Assuring the Availability of Critical Transportation Assets. GAO-08-851. Washington, D.C.: August 15, 2008.

Defense Critical Infrastructure: Additional Air Force Actions Needed at Creech Air Force Base to Ensure Protection and Continuity of UAS Operations. GAO-08-469RNI. Washington, D.C.: April 23, 2008 (For Official Use Only).

Defense Critical Infrastructure: DOD's Risk Analysis of Its Critical Infrastructure Omits Highly Sensitive Assets. GAO-08-373R. Washington, D.C.: April 2, 2008.

Defense Infrastructure: Management Actions Needed to Ensure Effectiveness of DOD's Risk Management Approach for the Defense Industrial Base. GAO-07-1077. Washington, D.C.: August 31, 2007.

Defense Infrastructure: Actions Needed to Guide DOD's Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure. GAO-07-461. Washington, D.C.: May 24, 2007.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548